Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claims 1-16 (canceled).

Claim 17 (currently amended). A method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from a device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data; ~~and~~

sending the digital signature of the device to an authentication server; and

determining whether the device has been excluded from accessing or enrolling in the service.

Claim 18 (previously presented). The method of claim 17, wherein the digital signature sent to the authentication server is encrypted.

Claim 19 (previously presented). The method of claim 17, wherein the software agent is installed on the device as part of the process of using the device to access a service.

Claim 20 (previously presented). The method of claim 17, wherein the hashes used to generate the digital signature are changed with every attempt to access a service, and the hashes cannot be reversed.

Claim 21 (previously presented). The method of claim 17, wherein the digital signature is one of several stages of a framework of authorization and authentication processes governing access to the service by the device.

Claim 22 (previously presented). The method of claim 17, wherein the authentication server compares the digital signature sent with one or more previously-stored digital signatures.

Claim 23 (currently amended). The method of claim 17 ~~22~~, wherein the authentication server determines whether the device has been excluded from accessing or enrolling in the service by determining whether the device is on a list or in a group of devices not allowed to access the service, or is included within a group of devices allowed to access the service.

Claim 24 (currently amended). The method of claim 17 ~~22~~, wherein the authentication server allows a maximum number of enrollments for a particular device.

Claim 25 (previously presented). The method of claim 24, wherein the maximum number of enrollments is zero.

Claim 26 (previously presented). The method of claim 22, wherein the authentication server allows minor modifications to the software or hardware configurations of a previously-enrolled device so as to preserve access or denial of access for the device.

Claim 27 (previously presented). The method of claim 26, wherein the previously-stored digital signature of the device is updated to reflect the modifications.

Claim 28 (previously presented). The method of claim 17, wherein the authentication server logs all accesses or attempted accesses by a device to the service.

Claim 29 (previously presented). The method of claim 17, wherein multiple devices can be registered for a single user with the authentication server to create a registration hierarchy.

Claim 30 (previously presented). The method of claim 29, wherein a user can unregister a device only through the device itself, or another device within the registration hierarchy registered earlier than the device to be unregistered.

Claim 31(currently amended). A method for identifying devices and controlling access to a service, comprising the steps of:

collecting data related to software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server;

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero;

and registering the device as authorized to access the service

~~registering a device with an authentication server for access to the service; and~~

~~verifying the identity of the device each time it subsequently attempts to access the service.~~

Claim 32 (currently amended). The method of claim 31, further comprising the step of verifying the identity of the device each time it subsequently attempts to access the service ~~wherein the step of registering a device comprises the steps of:~~

~~collecting data related to software and hardware configurations from the device through a software agent;~~

~~generating a digital signature for the device by hashing the software and hardware configuration data;~~

~~sending the digital signature of the device to the authentication server;~~

~~verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero;~~

~~and registering the device as authorized to access the service.~~

Claim 33 (currently amended). The method of claim 32 ~~31~~, wherein the step of verifying the identity of the device comprises the steps of:

collecting data related to current software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

comparing the digital signature sent with one or more previously-stored digital signatures for the device.

Claim 34 (currently amended). The method of claim 32 ~~31~~, wherein the step of verifying the identity of the device comprises the steps of:

collecting data related to current software and hardware configurations from the device through a software agent;

generating a digital signature for the device by hashing the software and hardware configuration data;

sending the digital signature of the device to the authentication server; and

verifying that the device is not on a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.

Claim 35 (currently amended). A system for identifying devices and controlling access to a service, comprising ~~the steps of~~:

a software agent installed on a device, adapted to collect data related to software and hardware configuration of the device;

a digital signature for the device, generated by the software agent by hashing the software and hardware configuration data; and

an authentication server that determines whether the device can access the service based upon the digital signature of the device;

wherein the authentication server verifies that the device is not a list or in a group of devices not allowed to access the service, or is not a device with a maximum number of enrollments set to zero.